REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
28-08-2012	Related Material	-

4. TITLE AND SUBTITLE
Hacking Facebook Privacy and Security

5a. CONTRACT NUMBER
W911NF-11-1-0174

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
206022

6. AUTHORS
Dr. Jeff Duffany (Advisor), Omar Galban

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
Polytechnic University of Puerto Rico
377 Ponce De Leon
Hato Rey
San Juan, PR 00918 -

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
58924-CS-REP.7

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT
When people talk about hacking and social networks, they're not referring to the common definition of hacking, which is using malicious code or backdoors in computer networks to damage systems or steal proprietary information. Hacking into social networks requires very little technical skill. It's much more of a psychological game using information on personal profiles to win a complete stranger's trust. Facebook offer privacy settings for their users but they don’t the give the users a simple and easier way to edit them or use them.

15. SUBJECT TERMS
Facebook, Privacy, Security, Social Network

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Alfredo Cruz
UU	UU	UU	UU		19b. TELEPHONE NUMBER 787-622-8000

Report Title

Hacking Facebook Privacy and Security

ABSTRACT

When people talk about hacking and social networks, they're not referring to the common definition of hacking, which is using malicious code or backdoors in computer networks to damage systems or steal proprietary information. Hacking into social networks requires very little technical skill. It's much more of a psychological game using information on personal profiles to win a complete stranger's trust. Facebook offer privacy settings for their users but they don’t the give the users a simple and easier way to edit them or use them.

Hacking Facebook Privacy and Security

Omar Galban
Computer Engineering
Jeffrey Duffany, Ph.D.
Computer Engineering Department
Polytechnic University of Puerto Rico

Abstract *— When people talk about hacking and social networks, they're not referring to the common definition of hacking, which is using malicious code or backdoors in computer networks to damage systems or steal proprietary information. Hacking into social networks requires very little technical skill. It's much more of a psychological game using information on personal profiles to win a complete stranger's trust. Facebook offer privacy settings for their users but they don't the give the users a simple and easier way to edit them or use them.*

Key Terms *— Facebook, Privacy, Security, Social Network*

INTRODUCTION

Online social networking communities have undergone an explosion in recent years, as both the kinds and numbers of sites has grown and membership increased. As part of their participation in online communities, Internet users are revealing a large amount of personal information [1]. This proliferation of personal data presents a variety of risks for individuals; such as identify theft, stalking, embarrassment, and blackmail. As participation in online communities increases, so does the necessity for flexible privacy mechanisms to protect user data. Despite these risks, many privacy mechanisms of online social communities are purposefully weak to facilitate joining the community and sharing information. Additionally, there is little awareness and use of existing privacy mechanisms among active users. Research has offered several explanations for this under-utilization of privacy options, including poor interface design, permissive default settings, social conformance, and inherent trust in the online community. In many cases, users are unwilling or unable to put forth the effort to modify and manage their privacy settings to protect their personal information. The aim of this investigation is to ask us two question, what can hackers do to protect the privacy of the 800 million Facebook users? And can we trust Facebook privacy settings? This research, we will see the different privacy settings options that Facebook has to offer and how to use it, finally we will test the settings using my Facebook account and a dummy Facebook account to see how the Facebook privacy settings actually work.

BACKGROUND

Privacy is an inevitable issue for Facebook [7]. It has become much easier these days to find almost any person's personal information through online technologies with search engines such Google and Bing. Social Network Sites provide the next big step forward invading users' privacy because users willingly post personal information either without considering the consequences or believing that their information is somehow protected. However, practically this is not always the case and privacy on social networking sites has received more attention from individuals in many fields of study.

Facebook has become increasable popular among teenagers who can easily become victims of privacy invasion because of lack of awareness of privacy issues. Causing members of this group reveal more information on the Facebook profile page than older users. This lack of awareness can lead to unexpected consequences. Many researches have addressed this issue by proposing three approaches to solve this problem: Social, Technical, and Legal [2]. On the other hand, we can evaluate the possibility that Facebook may be used

as a way to transmit personal information that many people that they dare not do it personally.

FACEBOOK PLATFORM

Facebook is a popular social networking site with over eight hundred million users and counting [2]. Users can see the profiles of their friends and network (e.g. College) members. Profiles include photos, dating preferences, birthdays, etc. Since the launch of the Facebook Platform, profiles can also display third-party gadgets. On the Facebook network, there were approximately 500,000 Facebook applications, and it attracted 1,100 developers daily [3]. Three reasons may account for this. Firstly, using the open platform, advertising firms can exploit social graph of users to have a clearer understanding demographic of the users, so it is shown to be effectively way to distribute information to potential customers using the social graphs. Secondly, developers can develop applications quickly on the Facebook platform, making it attractive from a profit measure. Thirdly, the platform is available in many programming environments, such as PHP, ASP, Java, C, C++, and Python, so the developers can select their comfortable environments.

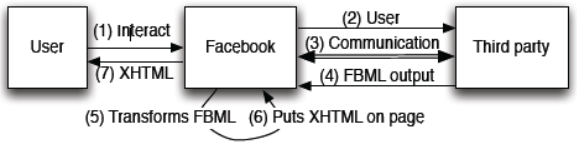

Figure 1

Shows third party content is integrated into profiles

In Step 1, a user interacts with an application's homepage through the Facebook website. The Facebook server passes the user's ID and session key to the third party (Step 2). The application running on the third party's server requests data from Facebook servers through a representational State Transfer (REST) interface. Querying the server requires a valid user session key and application secret. Applications can request detailed information about the user, the user's friends, and members of the user's networks. In Step 4, the application sends its output back to the Facebook server for display. See Figure 1 for more information. Using the Facebook API, applications can access a database of information as given in Table 1 can be considered as sensitive information for some users. The complete list can be found at Facebook: Facebook developer's Technical report, Facebook.com (2007) [4].

Table 1

Application developers' access to user's personal information

Tables	Description
user	User profile information first name, last name, birth day, sex, hometown location ,political preference, religion, work history ,education history, interest, activities, etc.
friend	All friends or a user. Facebook API method returns list of user IDs (uid).
group	Groups a user belongs to along with group IDs, names, group types, and descriptions.
group member	Member list of a specific group.
event	Upcoming event organized by group or friend along with that event's unique ID.
event member	Invited member's status of an event.

FACEBOOK ACCOUNT SETTINGS

ID fraudsters target Facebook and other social networking sites to harvest information about you. Here's how we recommend you set your Facebook privacy options to protect against online identity theft. For starters Facebook privacy settings or other settings are found in the right upper corner of the facebook main page, right beside the your name account. See Figure 2. When the user clicks the account settings it will bring you to the Edit profile page when you can access some hidden privacy features for example if you want that only friends see your basic information or if privacy does not matter to you go for the Public feature. With the public feature selection means that everyone in the

facebook world will see your basic information. This hidden Facebook privacy edit profile feature contains the following information : Basic Information, Profile Picture, Friends and Family, Education and work, Physolophy, activities and contact information. This information is the basic information thay you put when you first sign-up for Facebook, and Facebook don't even bother to tell users that you can edit those feature and put some privacy settings that all users can use to protect their data and personal information.

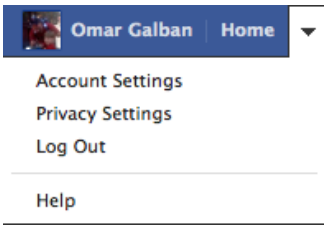

Figure 2
Facebook Privacy settings menu

FACEBOOK PRIVACY SETTINGS

The second option that Facebook give us is the privacy settings for your account, when you press the privacy settings button or link, it will bring up the privacy settings page. As you can see in Figure 3, Facebook mention that you can manage the privacy of your status updates, photos and information using the inline audience selector when you share or afterwards.[5] It also give you the chance to try out the privacy settings to see if you like or not before make it official. In the next section you will get to know what kinds of features can be edit and see how the privacy settings work.

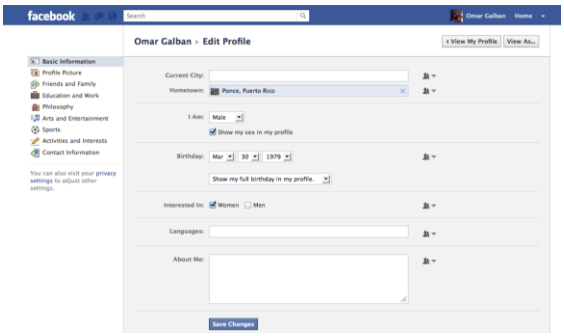

Figure 3
Account and Privacy Setting Screen

FACEBOOK PRIVACY SETTINGS FEATURES

If you take a look on Figure 3 you will notice that the privacy settings are divided as follow:

- Control Your Default Privacy- This setting will apply to status updates and photos you post to your profile from a Facebook app that doesn't have the inline audience selector, like Facebook for Blackberry or other mobile devices. Audience selector is facebook newest feature that provide users with an option of who can see what you post or updates in Facebook, by default this setting is set to Public. This setting has three options: Public, Friend and Custom. If you choose Public, the system will make all wall post,personal information, photos and video automatically available for everyone on the facebook world, meaning a high risk in terms of privacy or online thefting. If you choose Friends it will automatically set all available photos,video and wall post available only for your accepted friends. The last one is Custom, when you select custom it gives the user the oportunity to select who can see your information and hide from unathorized users. See Figure 3 for more information.
- How you connect - Control how you connect with people you know. It contains who can look up you up on facebook, who can send you friend request, who can post in your wall and Who can see Wall posts by others on your profile. For each of these questions Facebook offers three options: Everyone, Friends of Friends, and Friends. By default all three options are set to Everyone. See Figure 4.
- How Tag works - Control what happens when friends tag you or your content. This option provides a lot of functionality for Facebook users, for example, let's say that someone you know a friend, and post something on your wall that you don't

want him to post. When you use this option, you can select if you want to review other people post on your wall if you like approve it and that's it. When you use this function a pending post link will be available for you on your profile page. You can enable or disable this feature. Another nice feature in the how tag works is the photo tagging, lets say that you were in a party and some of your friends take some crazy pictures from you and you don't want to be tag in that picture, well with this feature you will be able to approve or decline that photo tag. Giving you the opportunity of control what other people post photos related to you. One feature that is available and for me is the most important one is the check-in tag. This feature is the most dangerous tagging of all because it bring the opportunity for other people to tag you when you are in a place with them, this is the most tag use on facebook, it provide sufficient information to a thief or relative one to know that you are currently away from home. This feature can be turn on or off in this section. See Figure 5.

- Apps and Websites - Control what gets shared with apps, games and websites. This setting is the most important of all setting in my personal opinion. This settings does not exactly provide the privacy that facebook users needs, when you install or accept to install an application within Facebook, Facebook warns you that the application will access all your profile basic information for example gender,age, town, age etc. currently there is no way to deny the access of application to that extremely sentitive information. This Facebook most critize feature, it give the chance to malicious developers or marketing companies to obtain personal information about you and use it to make some profit or using for marketing purposes. The Apps and websites setting can give you the chance to remove that installed application and tell you how what kind of information is required for the application to work. Is highly recommended that if you don't need or use that application remove it inmediatltly See Figure 7.
- Public Search - Show a preview of your Facebook profile when people look for you using a search engine. Many of users including myself want to search for old friends on the intenet, when you use google and do a search for a friend is highly probable that you will find it using Facebook, when you click of that forgotten friend, Google will show his Facebook Profile Search with all his personal information available to anyone without the user authorization, Facebook give the opportunity to edit that search on google to disable any search engine to look up on you on Facebook. See Figure 6.

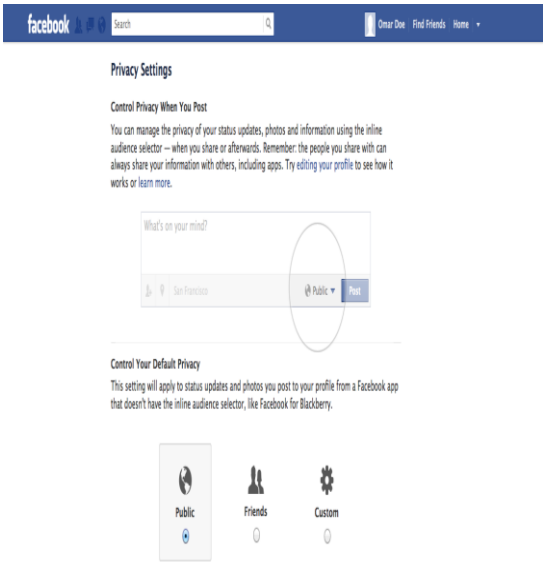

Figure 4
Privacy Setting Screen

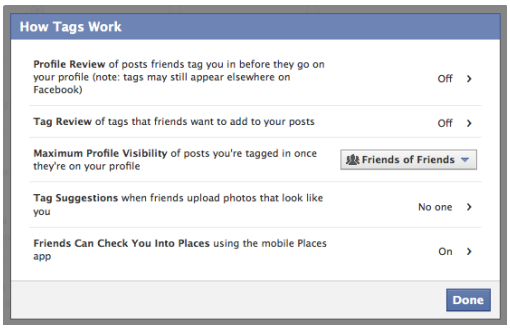

Figure 5
How Tags Work

Figure 6
Public Search Screen

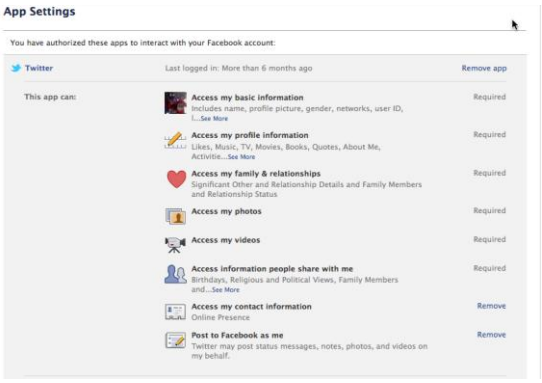

Figure 7
App Settings

FACEBOOK TIMELINE FEATURE

Facebook's new Timeline has the potential to expose status updates and wall posts from years ago. Here's how you need to update your privacy settings before you or Facebook publishes your Timeline. If you care to keep your past in the past, Facebook's new version of the profile, called Timeline, makes that a little more difficult [8].

To switch to the new profile, go to Facebook's Introducing Timeline page and click "Get It Now." Otherwise, you can wait until you see an announcement with instructions at the top of your profile.

With Timeline, every status update, wall post and photo ever posted since the day you joined Facebook becomes easily searchable to you and your friends. For many early adopters especially dredging up the past for all to see could be a privacy nightmare.

When you or Facebook migrates your account to the new Timeline, you'll have one week to make adjustments to your past posts and privacy settings before your Timeline will go live for everyone to see. You can publish your Timeline yourself anytime within the seven-day waiting period.

Here's a look at what your options are for adjusting your settings, based on the level of privacy you want to achieve:

- How to make all posts friends-only. It's possible that your past posts have varied privacy settings based on when they were posted. One way the easiest of them all is to use one of the blanket privacy settings introduced not long ago: "Limit the Audience for past Posts. You'll find this option near the bottom of your Privacy Settings page. See Figure 8.

Figure 8
Timeline Limit the Audience

If you decide to use this option, the content on your Timeline that you've shared with more than your friends such as public posts will automatically change to Friends only. With this setting, though, people who are tagged and their friends will still are able to see the post.

- Limit the posts by others on your timeline. Another way to hide past posts is to limit specific people or lists of people from viewing what others have posted to your wall. To do this, go to your Privacy Settings page, then select "Edit Settings" next to "How You Connect." Select the

drop-down menu next to the last item "Who can see posts by others on your timeline?" and choose "Custom." See Figure 9.

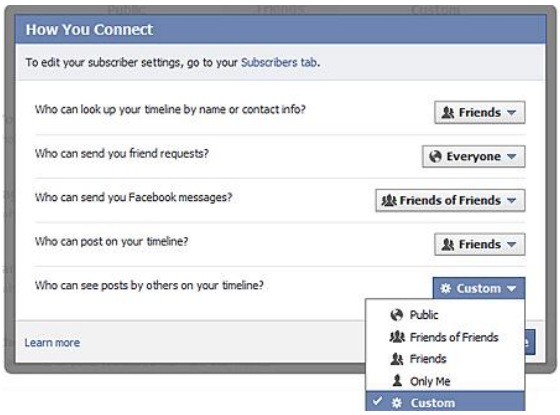

Figure 9
Timeline Posts

In the box under "Hide this from," type the names of the people or the lists that you want to exclude from viewing posts from others on your wall, for example those on your Limited Profile list. Then click Save Changes.

- Edit every post manually. I wouldn't recommend this option to anyone especially those who have been Facebook users for several years because of how time-consuming it could be. I wouldn't recommend this option to anyone especially those who have been Facebook users for several years because of how time-consuming it could be.

Your Timeline lets you search by the year, which breaks down into months. Hover over a story in the Timeline to hide a particular one this means that no one will be able to see it. See Figure 10.

While this is a tedious process, it does appear it's the only way to ensure you're hiding exactly what you want from the people you want. And there's always the "View Profile As" feature, which shows you what others see when they look at your profile.

Figure 10
Timeline Edit post manually

To find this feature after you've migrated to the new Timeline, click the gear icon on the right, below your cover photo, then click "View As." from the drop-down menu. To preview how your profile appears to the public, click the link in the text, or type a person's name into the field and click enter.

TESTING ACCOUNT & PRIVACY SETTINGS

One of the main purposes of developing this article is to answer a question. Can we trust Facebook privacy settings? For this experiment I used my Personal Facebook account, my wife personal account and created a dummy account to see how the settings interact. I created the account "Omar Doe" this user is new on Facebook and does not have any friends yet. To prove that when you sign-up on Facebook for the first time, the first thing that a normal user will do is to find their friends, most users forgot about privacy settings what you can actually share or insert on Facebook can be view by other people, people that are not your friends. The main problem is that initially Facebook Privacy settings are set to Everyone or Public. As you can see in figure , "Omar Doe" privacy settings are set to public ,any wall post, picture and personal information is available to the Facebook world and the user don't even know that. Using "Omar Doe" dummy account I post some messages in my wall with the followings privacy wall settings: post a message that's says "Hello World" with public feature, a second message saying "Testing Only me "feature and the third message saying "Testing friends" with the friend share feature. The results were as followed:

- Public Wall post – the message can be see by any user of Facebook.
- Only me post - The message cannot be see by any Facebook user including my friends. For this test I used my personal account and saw "Omar Doe" profile page.
- Friends Post – The message can be see by Omar Doe's friend. For this test my wife's Facebook account was used. My wife does not have "Omar Doe" as friend.

Omar Doe profile settings were modified to test the following scenario:

Only friends' setting was edited to basic information, city town, activities, work, and school. Using my wife Facebook profile, I did a search for Omar Doe, and enter his profile page. The Omar Doe's Profile page was indeed not sharing any basic information, city town, activities, work and school. However Facebook do not completely provide privacy settings for Friends. Facebook has a privacy setting for controlling who can see their friends. I select that only my friends can see Omar Doe friends and Facebook did it right but when I search for Omar Doe using my wife's account, Friends from Omar Doe was indeed invisible, but if you look closely on the Omar Doe info page, you can see that Omar Galban is indeed a friend of Omar Doe by seeing Omar Doe profile page using my wife account. See Figure 11. This is a serious bug on the system. You can actually see another people friend by being a mutual friend of the target member. Another important result is that as soon a known friend has beed added to your profile, a new list will be populated with almost all friends that the current user has, its called the "people you may know" feature. This list will recopilated all your friends and presented it to your newest friend, that way it will give the chance to find lost friends or to know how many friends the other user has. In the next section we will talk about third party applications that are been developed and implemented to aid users.

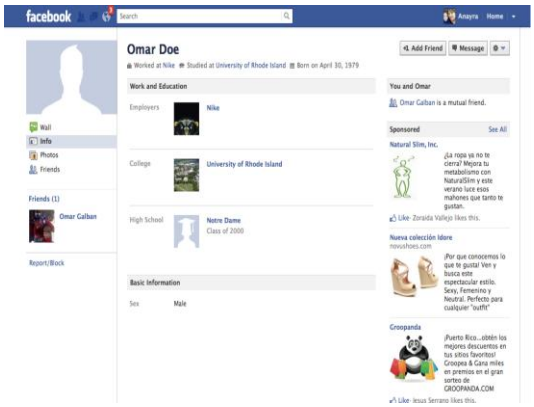

Figure 11

Mutual Friends Issue

PRIVACY PROTECTION SYSTEMS

For people or users that still does not trust Facebook at all, there are several browser extensions, application and websites that have been develop and implemented to protect privacy on Facebook, for example:

- *Reclaim Privacy.org*

  This app is a utility that runs while you're logged in to Facebook and looks over your privacy and profile settings to make sure your settings are configured to protect your data from prying eyes, advertisers, or partners who use apps and games to collect information about you. The scanner comes in the form of a bookmarklet that you click once you're logged in, and a frame will open at the top of your Facebook screen that shows which settings are configured securely and which areas have information about you available to the public.
- *Green Safe*

  This Facebook Application allows a person to display their personal info to their friends but protect it from partner sites and application developers. The aim of this app is that it will put users in control of their personal data. This application works storing and displaying your info for you allowing you to delete all

your personal info from Facebook where others may have access to it.

The use of this application and/or websites is recommended due to the fact that one of Facebook biggest problem is not the platform applications is the users awareness that privacy settings are available and people do not know that they exist, so the use of the website Reclaim Privacy.org is a great alternative to work on what Facebook privacy settings has to offer. Other applications such as browser extensions offer the users a privacy protection external by Facebook, the browser extension is called Anti Social for Firefox, this tool is an extension that protects the privacy of the Facebook users. It provides additional privacy controls and features to the user by preventing external sites from including Facebook content.

CONCLUSION AND FUTURE WORK

At this time when Facebook and social network are changing, new companies are trying to enter in the social network business to have a more clear perspective of what the users really want in terms of what music they hear and love or what comedy movie or action film is on the most wanted list an example of this is Spotify a music service and Netflix a blockbuster streaming moving service that Facebook now or will be introduce into the social life. Million of users are still signing to this social network, without the knowledge or awareness that everything that you share or write or even upload a picture can be access by malicious hacker or any normal people because of Facebook poor management of explaining the users how they can interact with their settings. Maybe Facebook wants to be that way because it will beneficial marketing companies to see what exactly a 800 million users and counting likes or will like to purchase, they can produce metrics and reports. To attend this problem I review,explaint and test many Facebook privacy settings to create an aawareness to users that be careful what you share, nobody knows if another user (who is not your friend) is following you to collect priviledge data. As far of my results I can say that Facebook Privacy settings works as expected but we need to extra careful and monitor those privacy settings once in a while. Three Facebook accounts were used to test those settings their scenario and results can be found in this article. One of the biggest problem that Facebook is having right know is the third party applications i.e gaming apps or utilities apps. Facebook does not truly provide any secure and privacy setting to handle applications; So, one recommendation is to research some new privacy protection settings or new privacy protection systems that will be embeded on the Facebook API. Facebook is trying to keep up with other social network such as Google +, with new ideas and better management of what people post or share in their Social Network [6]. Many Google + privacy and security settings are being copied by Facebook like circles. “Circles” enables users to organize contacts into groups for sharing across various Google products and services. Although other users can view a list of people in a user's collection of circles, they cannot view the names of those circles. The privacy settings also allow users to hide the users in their circles as well as who have them in their circle, in facebook is called friend list. Facebook is contansly changing their setting to “provide”more flexibility to users but let us remind that Facebook is a business so they will still find a way to expose people personal information; So maybe we haven’t seen yet the power of Facebook.

ACKNOWLEDGMENT

This research project would not have been possible without the support of many people. I would like to express my gratitude to my supervisor, Prof. Jeffrey Duffany who was abundantly helpful and offered invaluable assistance, support and guidance. Special thanks to God who guided me on this crazy journey, Also I would like to thanks my wife Anayra , my son Luis Omar, my best friend Marcus and to my family for their understanding & endless love, through the duration of my masters. We Did It!

REFERENCES

[1] Hargittai, E.: Whose space? differences among users and non-users of social network sites. Journal of Computer-Mediated Communication 13(1) 2008

[2] Boyd,D.: Why Youth (Heart) Social Network Sites. Massachusetts Institute of Technology, Cambridge, MA (2008)

[3] Facebook: http://www.facebook.com/press/info.php?statistics (2011)

[4] Facebook: Facebook developers. Technical Report, Facebook.com (2007)

[5] Facebook: Facebook, "Privacy Policy," http://www.facebook.com/policy.php (2010).

[6] Google Plus vs Facebook – An overview. http://www.faceblogger.com/google-plus-vs-facebook/ (2011)

[7] Facebook acknowledges privacy issue with third party applications. http://latimesblogs.latimes.com/ 2010/10/facebook-acknowledges-privacy-issue-with third-party-applications.html

[8] Facebook's New Timeline: Important Privacy Settings to Adjust Now. http://www.cio.com (2011)